情報処理学会論文誌 Vol.53 No.9 2094–2106 (Sep. 2012)

端末連携認証システムの開発と評価

梅澤 克之[1,a)] 礒川 弘実[2] 加藤 崇利[2] 萱島 信[2] 手塚 悟[3]

受付日 2011年11月16日, 採録日 2012年6月1日

概要：携帯電話やスマートフォンなどの携帯端末を利用し外出先から業務を遂行するモバイルワークが増えてきている．モバイルワークから通常業務（あるいはその逆）に業務体系を切り替える際に，モバイルワーク用の携帯端末を「鍵」として用いて，その携帯端末を他の端末にかざすだけで利用者認証が行えると便利である．さらに外出中には，不特定多数のユーザが利用できる端末（公共端末）が使えればより業務効率の向上が期待できる．本論文では，認証情報としての ID/パスワードや Cookie 情報を携帯端末から他端末に引き継ぐことによって，認証を簡略化する方法を提案する．さらに，引継ぎ先の端末が公共端末のような必ずしも安全性が確保されているとは限らない端末の場合には，公共端末が定期的に既存ツールを用いて自端末のウィルスやマルウェアをチェックし，チェック結果や自端末のインベントリ情報を偽造や改ざんができない方法で端末管理サーバに伝達させる．それらの情報をもとに端末管理サーバが公共端末の信頼性を判定し，判定結果を公共端末の画面に通知する．ユーザが視認することで公共端末の信頼性を確認し，安全であることが分かった場合のみ認証情報を連携させる方式を提案する．このような提案に基づいたシステムを開発し性能を評価する．これにより，ユーザは携帯電話を別の端末にかざすだけで認証が行われサービスを受けることが可能になる．

キーワード：携帯端末，公共端末，認証，端末連携，Bluetooth

Development and Evaluation of Federated Authentication System

Katsuyuki Umezawa[1,a)] Hiromi Isokawa[2] Takatoshi Kato[2]
Makoto Kayashima[2] Satoru Tezuka[3]

Received: November 16, 2011, Accepted: June 1, 2012

Abstract: Recently, the number of people performing mobile work on mobile terminals (MT) has increased. It is convenient to be able to perform user authentication by simply swiping over other terminals, using a MT as a "key." It is even more convenient if we can use public terminals (PT) outside of the company. In this paper, we propose a system that uses MTs as storage devices for authentication information such as IDs, passwords, cookie information, etc. by connecting MTs and various terminals through short distance wireless telecommunications. Additionally, a PT checks itself for viruses and malware regularly by using an existing tool and safely transmits the check result and inventory information to a terminal management server (TMS). The TMS judges the reliability of the PT by using this information and notifies the PT of the result. The user sees the result and confirms the reliability of the PT. Authentication information is transferred to the PT only when the user acknowledges that the PT is safe. Furthermore, we developed this system based on our proposal and evaluated its performance. As a result, users could receive a service on a terminal simply by swiping the MT over it.

Keywords: mobile terminal, public terminal, authentication, federation, Bluetooth

[1] 日立製作所情報システム事業部
Information Technology Division, Hitachi, Ltd., Chiyoda, Tokyo 101–8010, Japan
[2] 日立製作所横浜研究所
Hitachi, Ltd., Yokohama Research Laboratory, Yokohama, Kanagawa 244–0817, Japan
[3] 東京工科大学コンピュータサイエンス学部
School of Computer Science, Tokyo University of Technology, Hachioji, Tokyo 192–0982, Japan
[a)] katsuyuki.umezawa.ue@hitachi.com

1. はじめに

1.1 背景

近年，携帯電話の保持率は１人１台以上になっている．また，個人所有だけではなく公共端末なども含めて，様々な端末を使って様々なサービスが受けられるようになってきた．サービスを受ける際にはユーザ認証が重要である．ユーザ

認証の際に，個人が所有する携帯端末を「鍵」として利用できれば便利である．たとえば，ID/パスワードの保管庫として用いて，携帯端末を PC にかざすだけで Web のフォームへ自動入力がなされると便利である．また，認証用のハードウェアトークンや決済用の IC カード，カーシェアリング向けの乗用車の鍵としての各役割を携帯端末が果すことで，ユーザの利便性が大きく向上することが期待できる．

本論文では，このようなユースケースを実現するための携帯端末を認証情報の保管庫として用いる端末連携認証システムの提案を行う．具体的には，認証情報としての ID/パスワードや Cookie 情報を携帯端末から他端末に引き継ぐことによって，認証を簡略化する方法を提案する．さらにその際に，認証情報を引き継ぐ先の端末の信頼性を確認し，安全であることが分かった場合のみ認証情報を連携させる方式を提案する．公共端末の信頼性の確認は，公共端末の状態を定期的に端末管理サーバに送信し，端末管理サーバが公共端末の信頼性を判定し，ユーザに公共端末の信頼性を示す方式で行う．具体的には，公共端末が自端末内のウィルスやマルウェアを既存のツールを用いてチェックする．さらにパターンデータが最新になっていることや不適切なアプリケーションがインストールされていないことを確認するための自端末のインベントリ情報を取得する．公共端末から定期的にウィルスチェック結果やインベントリ情報を端末管理サーバに偽造や改ざんができない方法で伝達し，端末管理サーバが公共端末の信頼性を判定する．判定結果は，端末管理サーバから公共端末に通知され，ユーザは公共端末の画面に表示される情報を視認し，公共端末が信頼できる状態にあること（事前に設定・登録したユーザ情報と相違ない情報を端末管理サーバが送ってきたこと）を確認し，「継続/中止」を選択する．「継続」が選択された場合のみ認証情報を携帯端末から公共端末に連携させる．「中止」を選択した場合には，信頼性の確認ができていない公共端末に認証情報を盗まれることはない．このような提案に基づいたシステムを開発し性能を評価する．

以下では，まず，一般的な利用イメージを想定して提案のモチベーションを示したうえで，2 章で提案の準備として，関連研究，提案方式のモデル化，および前提条件を示す．3 章で ID/パスワードや Cookie 情報を携帯電話と PC 端末間で転送しあう提案方式について示す．4 章で性能の評価を行い，5 章で実運用に向けた考察を行う．最後に 6 章でまとめと今後の課題を示す．

1.2 提案のモチベーション

図 1 に PC 端末を使って Web アクセスを行う際の利用シーンを示す．図 1 に示したように，現状では様々なサービスに対して個別に ID が振られて，それぞれの ID ごとにパスワードの入力を行う必要がある．また，サービスのポリシによっては短期間で別のパスワードへの変更を強制される場合もある．このように多数の ID とパスワードを覚えておくことはかなり難しい状況にある．これに対して Web ブラウザに覚えさせてしまう方法もあるが，多人数で利用する共用端末（以降，公共端末と呼ぶ）などでは，ユーザが変わるごとにキャッシュをクリアするなどの運用を行わないとキャッシュしたパスワードを勝手に利用されてしまう場合がある．そこで個人が所有する携帯端末に ID/パスワードを覚えさせて，PC にかざすことで，PC の安全性を確認したうえで ID/パスワードを渡すことで利便性と安全性の向上が期待できる．

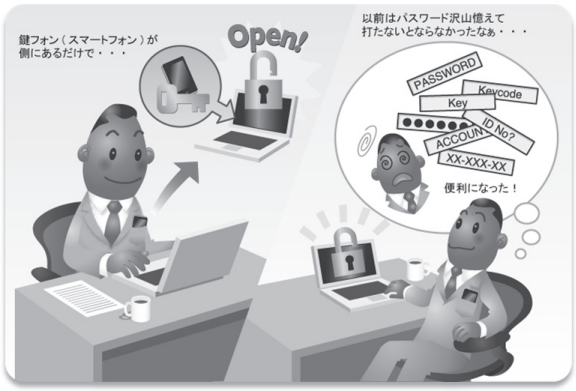

図 1 携帯端末が認証情報の保管庫に
Fig. 1 Mobile terminals become storage of authentication information.

図 2 PC 端末での業務を引き継ぐ
Fig. 2 They can work with PC sequentially.

図 2 に外出先での利用シーンを示す．外出先では利用場所の制限などにより携帯端末単体での利用が好ましい場合がある．このときにも外出前に行っていた作業を継続したいという要求や，再認証手続きを簡略化したいという要求が強い．

図 3 に携帯端末を認証トークンとして用いることの利点を示す．たとえば PC 端末が置き引きにあったとしても，鍵としての携帯端末が同時に盗まれなければ，PC 端末は利用できない．また，携帯端末を単体で盗まれたとしても，携帯端末の GPS 機能での追跡や，サーバ経由でリモートデータ消去が行えるため，携帯端末は失くしても安心な認証トークンになりうる．

図 3 携帯端末を失くしても安心
Fig. 3 Correct even if terminal is lost.

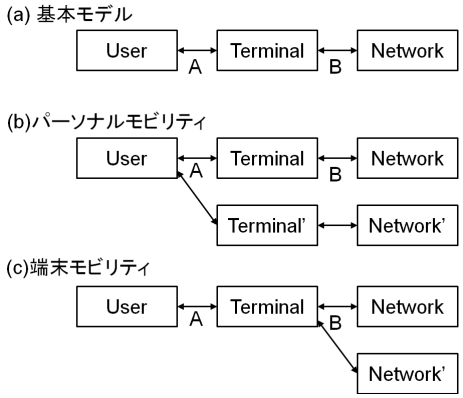

図 4 文献 [1] に定義されている構成要素間の関係
Fig. 4 Relations between elements shown in Ref. [1].

2. 提案の準備

2.1 関連研究

文献 [1] にユーザと端末が移動する際のシームレス通信サービスの分類定義がなされている．**図 4** (a) に示すように，「User」「Terminal」「Network」の 3 つエンティティとその間の関係「A」と「B」の変化によってモデルを抽象化している．その中で「A」の関係が変化するモビリティを「パーソナルモビリティ」（図 4 の (b)），「B」の関係が変化するモビリティを，「端末モビリティ」と呼んでいる（図 4 の (c)）．さらに「パーソナルモビリティ」に関しては，「ユーザモビリティ」，「プロファイルモビリティ」，「セッションモビリティ」の 3 種類に分類整理している．この中で「ユーザモビリティ」は自分専用ではない端末でもその個人がサービスを要求/着信していることが通信相手から分かるという定義がなされている．本論文は，文献 [1] における「ユーザモビリティ」の範疇の研究というように位置づけることができる．

「ユーザモビリティ」に関連する研究として，文献 [2] では，SIP forking proxy でメッセージを多重配信することでユーザモビリティの基盤を実現している．また，文献 [3] では，個人に 1 対 1 で対応するパーソナルプロキシを導入し個人への到達性を確保している．また，ICEBERG プロジェクト [4] では，Universal Inbox というサービスで，ユーザを iUID（iceberg Universal ID）で識別し，コンテンツをユーザの移動先に合わせた形式に変換して届けることを行っている．

上述の関連研究は，「ユーザモビリティ」のうちの着信に着目した技術である．これに対してサービス要求（認証）に着目した技術として，文献 [5] がある[*1]．文献 [5] では，外出先で携帯型受信機でコンテンツ視聴サービスを受け，帰宅後に，携帯型受信機の認証情報とサービス状態をテレビ受信機に引き継ぐ方式を提案している．具体的には，リバティアライアンスが提唱する ID-WSF（ID Web Service Framework）[6] を拡張し，アサーションと呼ばれる認証情報を複数端末間で移動させることにより端末連携を実現している．認証情報を端末間で移動するという考え方は，我々の提案と同様であるが，移動先（テレビ受信機）の安全性に関しては言及されていない．

また，我々は，携帯端末をセキュリティデバイスと見なして PC 端末と連携させてリモートアクセスを行うシステムの提案を行ってきた [7], [8], [9], [10]．しかし，これらの提案では携帯端末と PC 端末は個人の持ち物という前提でそれらの端末の組合せは固定的であった．たとえば共有 PC 端末を利用する場合などは動的な端末の組合せが必要とされていた．このような動的な端末の組合せを可能とし，いくつかの通信プロトコルに対応させる提案も行ってきた [11], [12], [13], [14]．文献 [7]～文献 [14] の提案に関しても，認証情報を引き継ぐ先の端末の安全性について考慮したものではなかった．

2.2 提案方式のモデル化

まず，提案方式をモデル化する．提案方式の基本モデルを**図 5** (a) に示す．これは，図 4 の「User」の概念をより具体的に IC チップのような「Secure Element」と携帯端末のような「Mobile Terminal」の 2 つのエンティティで書き直したモデルになっている．また，端末モビリティは考えないので，直感的に分かりやすいように図 4 の「Terminal」を「Fixed Terminal」と書き改めている．そして，本提案では，図 5 (b) のように「A」の関係が変化するモデルを扱う．ここで「Fixed Terminal」が存在しない場合も「A」の関係の変化ととらえて提案方式の対象に含めている．

2.3 前提条件

本節では，提案における前提条件を示す．

- 携帯端末は，個人が所有する端末であり信頼できるものとする．
- 携帯端末には，セキュアエレメントが装着され，携帯

[*1] 本文献にはユーザモビリティだけでなく，プロファイルモビリティも含まれている．

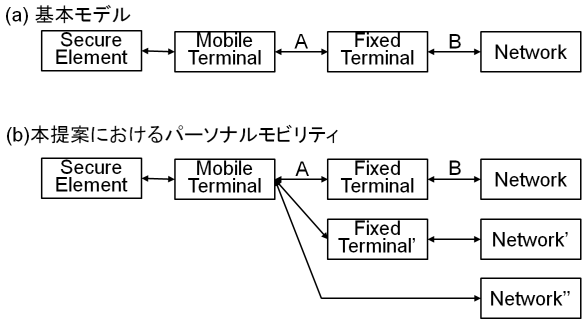

図 5 提案方式のモデル化
Fig. 5 Modeling of proposal.

端末とセキュアエレメント間の通信路は安全であるとする．

- セキュアエレメントそのものは耐タンパ性を有し，安全であるとする．
- 端末管理サーバは，適切な管理者が運用するため信頼できるものとする．
- PC 端末，公共端末は，鍵を保管しその鍵を使って暗号演算を行うことができるセキュアな領域を持つものとする．
- PC 端末は，企業内などで適切に運用され信頼できるものとする．
- 公共端末は，不特定多数の利用者が使用するため，ウィルスやマルウェアなどが混入する可能性があるものとする．つまり公共端末の信頼性は必ずしも確保できない状態になる可能性があるとする．ただし，公共端末は，自端末のウィルスやマルウェアの状態を既存のツールを用いてチェックすることができるものとする．また，ウィルスチェックのパターンデータが最新になっていることや，不正なアプリケーションがインストールされていないかなどの確認のために自端末のインベントリ情報（ソフトウェア情報やハードウェア情報）を正しく収集できるものとする．さらに，公共端末から定期的に送信されるインベントリ情報は偽造や改ざんができない方法で端末管理サーバに伝達できるものとする．
- 公共端末は，不特定多数の利用者が使用する端末を指す．たとえば，空港や駅などの公共の場やネットカフェなどに設置されている PC 端末などが含まれる．ATM などの専用端末は，機能を限定して信頼性を保っているので本論文の対象外である．
- 公共端末に割り当てられる端末 ID は，偽造できない ID 体系により生成されているものとする．
- 携帯端末，PC 端末，および公共端末の時刻はおおむね同期しているものとする．

3. 提案方式

3.1 提案方式の概要

本節では，認証情報を引き継ぐ先の端末の信頼性を確認し，安全であることが分かった場合のみ認証情報を連携させる方式を提案する．

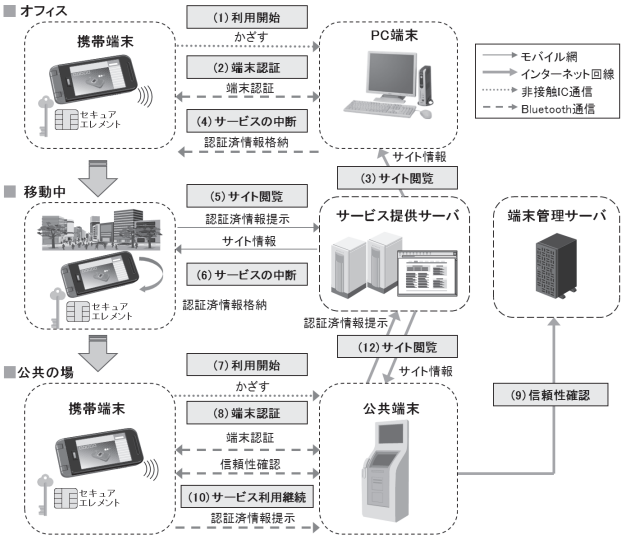

図 6 提案システムの全体概要
Fig. 6 Summary of proposed system.

本節では提案方式の全体概要について記述する．**図 6** に全体概要を示す．提案方式では図 6 に示すように，3 つの利用シーンを想定する．

- 携帯端末を PC 端末にかざすことによって ID/パスワードを転送し，Web のフォームへ自動入力しサービス提供サーバに自動的に接続する．1 度 Web 認証がなされると，サービス提供サーバ側から認証済情報としての Cookie が発行されるので，その Cookie 情報を携帯端末に保管する（図 6 の「オフィス」）．
- 携帯端末自身でサービスを受ける場合には，前記 Cookie 情報を自身のブラウザにセットし，サービス提供サーバに接続しサービスを受ける（図 6 の「移動中」）．
- 最後に，公共の場で，不特定多数のユーザが利用する端末（公共端末）でサービスを受ける（図 6 の「公共の場」）．不特定多数のユーザが利用する公共端末では，公共端末の安全性が確保されていない状態でパスワードや Cookie 情報を転送してしまうことはセキュリティ上問題がある．よって，携帯端末と公共端末で端末認証を行ったうえで，さらに，公共端末にウィルスやマルウェアが存在していないことを端末管理サーバで確認し，確認結果をユーザに通知することで公共端末の安全性を確認する．その後，携帯端末内に保管されている Cookie 情報を公共端末に転送し，公共端末のブラウザにセットし，サービス提供サーバに接続しサービスを受ける．

なお，図 6 の (2)，(8) の端末認証は，これらの端末どうしが提案方式のスキームに従っているかを確認するためであり，(9) の信頼性確認は，提案方式のスキームに従っている端末だとしても利用時に安全な状態になっているとは限らないため，その確認のために必要な処理である．

3.2 要求条件

本節では，提案における要求条件を示す．

- 携帯端末を他端末にかざすことで認証情報を委譲し，その認証情報を用いて認証処理を行える．
- 他端末が，公共端末のような不特定多数の利用者が使う端末であり，信頼性が確保できない場合でも，それを確認することができる．
- サービス提供機関は従来と変わらない仕組みでサービスを提供できる．
- 携帯端末単体でもサービスを受けることができる．

3.3 提案方式のシーケンス

本節では前節で示した 3 つの利用シーンについて，それぞれ下記に列挙するシーケンスについて詳細を示す．

- オフィスで，携帯端末を PC 端末にかざしてサービスを受ける．
- 移動中に，携帯端末でサービスを受ける．
- 移動先の公共の場で，携帯端末を公共端末にかざして，公共端末の安全性を確認する．
- その後，携帯端末内の認証情報を使って公共端末でサービスを受ける．

3.3.1 PC 端末利用のシーケンス

PC 端末に携帯端末をかざして PC 端末上でサービスを享受し，携帯端末に認証情報を連携するまでの処理フローを**図 7** に，その説明を**表 1** に示す．なお，本論文では，図 7 において，携帯端末から PC 端末への認証情報（ここでは，ID/パスワード）の送信があることを明示しているが，公共端末の信頼性が確認できた後であれば，後述の図 10 に示すように，携帯端末から公共端末への認証情報（ID/パスワードを含む）の送信は可能である．

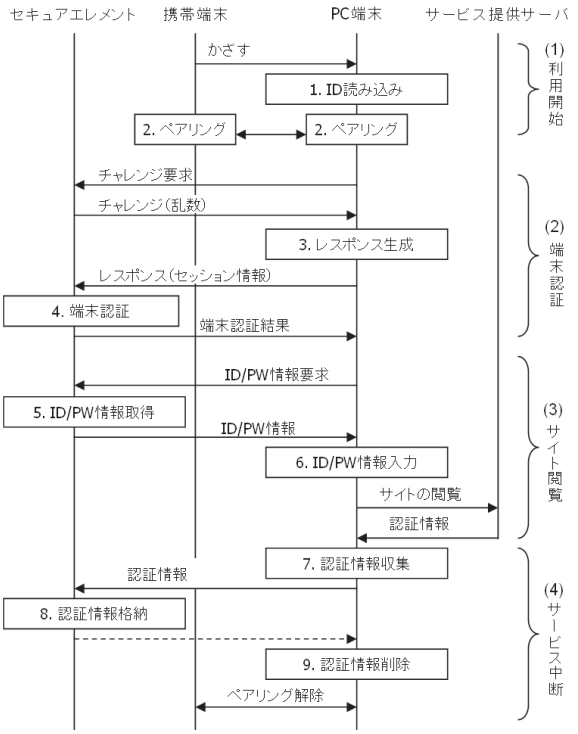

図 7 PC 端末利用のシーケンス
Fig. 7 Sequence when PC terminal used.

3.3.2 携帯端末利用のシーケンス

セキュアエレメントに格納されている認証情報を利用して，携帯端末上で引き続きサービスを享受する処理のフローを**図 8** に，その説明を**表 2** に示す．なお，携帯端末は個人利用を想定しているため信頼性確認は省略している．

3.3.3 公共端末の安全性確認のシーケンス

公共端末に携帯端末をかざして，公共端末の安全性を確認する処理のフローを**図 9** に，その説明を**表 3** に示す．

なお，図 9 および表 3 のステップ b において，公共端末のインベントリ情報を収集しているが，**表 4** に各種インベントリ情報の例を示す．また，図 9 および表 3 のステップ 9 において，端末管理サーバが各インベントリ情報を用いてどのような判定を行うかの例をあわせて示す．さらに，表 4 のインベントリ情報のうち，「ソフトウェア情報（アプリケーションの追加と削除の情報）」の例示を**表 5** に示す．

表 1 図 7 の説明
Table 1 Explanation of Fig. 7.

No.	説明
1	PC 端末に携帯端末をかざすと，PC 端末はかざされた FeliCa の ID を読み込む．
2	PC 端末と携帯端末間で FeliCa の ID をパスフレーズとして Bluetooth のペアリングを行う．
3	PC 端末は携帯端末のセキュアエレメントからチャレンジを取得し，PC 端末があらかじめ共有している共通鍵でチャレンジを暗号化したレスポンスを生成し，セキュアエレメントに送付する．なおレスポンスの生成は PC 端末のセキュアな領域で行われる．
4	セキュアエレメントは，チャレンジを共通鍵で暗号化した出力値と PC 端末から送付されたレスポンスを比較し，値が一致した場合は，端末認証成功と見なす．以降，本レスポンス値をセッション情報として保持する．
5	セキュアエレメントは，PC 端末からの要求に従い，ウェブサイトへログインするための ID/パスワード情報を PC 端末に送付する．
6	PC 端末は実行中のブラウザを検索し，ID/パスワード情報を入力し，PC 端末からサービス提供サイトにアクセスする．サイトから認証情報（Cookie）が発行され，サービスを受ける．
7	PC 端末は，自端末のブラウザが管理している認証情報を収集し，携帯端末に接続されているセキュアエレメントに送付する．
8	セキュアエレメントは受信した認証情報をセキュア領域に書き込む．
9	PC 端末は，自端末のブラウザが管理している認証情報を削除する．なお，携帯端末と PC 端末間の意図せぬ通信切断を考慮して，ステップ 7 の直後に認証情報を削除することで安全性を高められる．

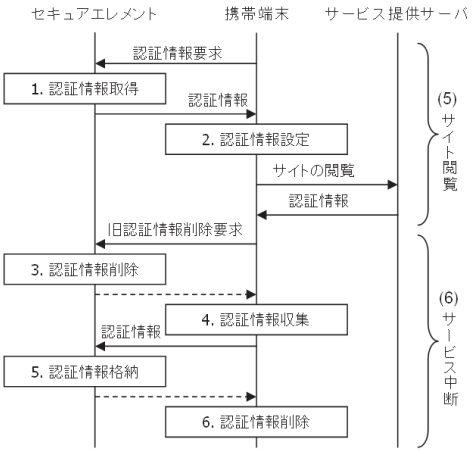

図 8 携帯端末利用のシーケンス
Fig. 8 Sequence when mobile terminal used.

表 2 図 8 の説明
Table 2 Explanation of Fig. 8.

No.	説明
1	セキュアエレメントは，セキュア領域内に格納している認証情報を取得し，携帯端末に渡す．
2	携帯端末は受信した認証情報をブラウザに格納し，サービス提供サイトにアクセスする．サイトから認証情報が発行され，サービスを受ける．
3	セキュアエレメントは携帯端末からの要求に従い，格納している旧認証情報を削除する．
4	携帯端末はブラウザが管理している認証情報を収集し，セキュアエレメントに渡す．
5	セキュアエレメントは認証情報をセキュア領域に書き込む．
6	携帯端末はブラウザが管理している認証情報を削除する．

3.3.4 公共端末利用のシーケンス

公共端末の安全性を確認したうえで，PC 端末から引き継いだ認証情報を引き渡し，公共端末上で引き続きサービスを享受する処理のフローを**図 10** に，その説明を**表 6** に示す．

3.4 公共端末の安全性確保処理の詳細シーケンス

本節で 3.3.3 項で示した公共端末の安全性確認シーケンスの詳細を図示する．図 9 のステップ 3〜ステップ 8 までの詳細を**図 11** に，図 9 のステップ 9〜ステップ 11 までの詳細を**図 12** にに示す．

まず，図 11 のステップ 3 とステップ 4 で端末どうしの相互認証を行う．公共端末は携帯端末のセキュアエレメントからチャレンジを取得し，公共端末があらかじめ共有している共通鍵でチャレンジを暗号化したレスポンスを生成し，セキュアエレメントに送付する．このレスポンスの生成は公共端末のセキュアな領域で行われる．セキュアエレメントは，チャレンジを共通鍵で暗号化した出力値と公共端末から送付されたレスポンスを比較し，値が一致した場

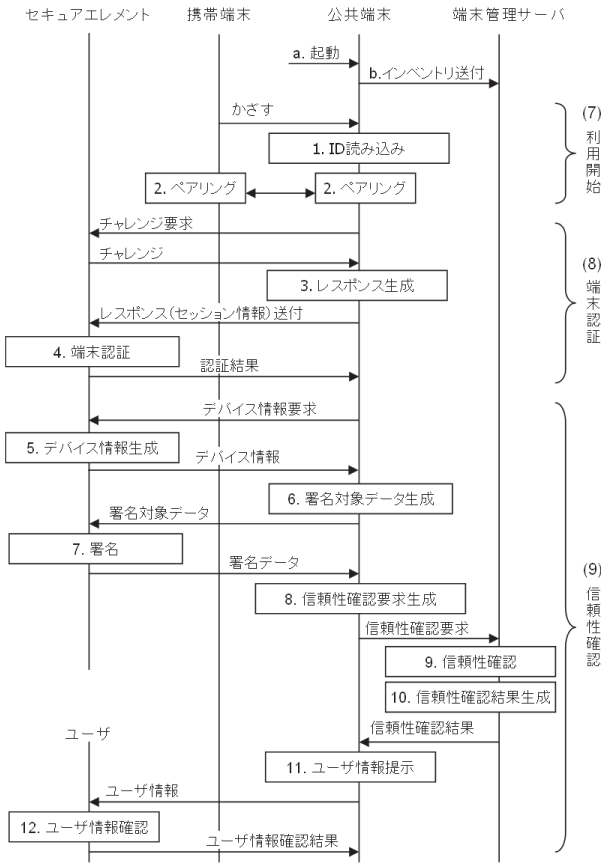

図 9 公共端末の安全性確認のシーケンス
Fig. 9 Sequence for safe confirmation of the public terminal.

表 3 図 9 の説明
Table 3 Explanation of Fig. 9.

No.	説明
a	信頼性確保モジュール起動する．
b	信頼性確保モジュールは自端末のインベントリ情報（インストールされているソフトウェア情報やハードウェア情報）を収集し，そのリストを定期的に端末管理サーバに送付する．
1	公共端末に携帯端末をかざすと，公共端末はかざされた FeliCa の ID を読み込む．
2	公共端末と携帯端末間で Bluetooth のペアリングを行う．
3〜4	端末認証を行う（詳細は，3.4 節を参照）．
5〜11	端末の信頼性確認を行う（詳細は，3.4 節を参照）．
12	ユーザは公共端末に表示された内容（公共端末が信頼できる状態にあるか否か）を視認し，事前に設定・登録したユーザ情報と相違ないことを確認し，続行/中止のいずれかのボタンを押下する．ユーザが「中止」を選択した場合には，処理は中断され，信頼できない公共端末に認証情報を盗まれる可能性はない．公共端末は，以降の処理におけるセキュアエレメントへのコマンドには，ステップ 18 で端末管理サーバがら受信した信頼性確認結果をコマンドに付加してセキュアエレメント内でその信頼性確認結果を検証することでセキュアエレメントへの不正なコマンド実行を防ぐことができる．

表 4 インベントリ情報の例示
Table 4 Example of inventory information.

インベントリ情報	判定方法
システム情報	端末の基本情報として判定に利用する．
ソフトウェア情報（アプリケーションの追加と削除の情報）	不適切なソフトが含まれていれば信頼できない端末と判定する．
ソフトウェア情報（ウィルス対策製品）	ウィルスワクチンソフト未対策であれば信頼できない端末と判定する．
ソフトウェア情報（非インストール型ソフトウェア情報）	不適切ソフト，不適切ファイルが存在すれば信頼できない端末と判定する．
システム構成情報	不適切ハードウェア構成であれば信頼できない端末と判定する．
ウィルススキャン実行結果情報	ウィルスやマルウェアに感染していれば信頼できない端末と判定する．

表 5 インベントリ情報（アプリケーションの追加と削除の情報）の具体例
Table 5 Specific example of inventory information (Addition and deletion of application).

ホスト名称	IP アドレス	ホスト識別子	パッケージ名称	パッケージ ID	状態	インストール日時
XX.jp	a.b.c.d	#Axx	Hotfix for Windows	Wxx-XXX	完了	’12/5/6
XX.jp	a.b.c.d	#Axx	Security Update	Wxx-XXX	完了	’12/2/8
XX.jp	a.b.c.d	#Axx	Anti-Virus Software	Wxx-XXX	完了	’12/3/1
XX.jp	a.b.c.d	#Axx	Update for 2007	Wxx-XXX	完了	’12/2/8
XX.jp	a.b.c.d	#Axx	Hotfix for Windows	Wxx-XXX	完了	’11/9/7

合は，端末認証成功と見なす．ここで共有鍵を使うことにしているが，公開鍵暗号に基づく方式にしてもよい．ここで保管されている鍵は，2.3 節の前提条件で示した「鍵を保管するだけのセキュアな領域」に保管されているものとする．この，端末認証により公共端末のすり替えを検知することができる．

次に，図 11 の残りのステップと，図 12 のすべてのステップで公共端末の信頼性確認を行う．まず，図 11 のステップ 5 で，セキュアエレメントは，デバイス情報を事前に保持している端末管理サーバの公開鍵で暗号化する．デバイス情報とは，セキュアエレメントの ID と，ユーザが事前に設定した任意の文字列であるユーザテキストと，ステップ 4 のレスポンス値（以降，セッション情報と呼ぶ）

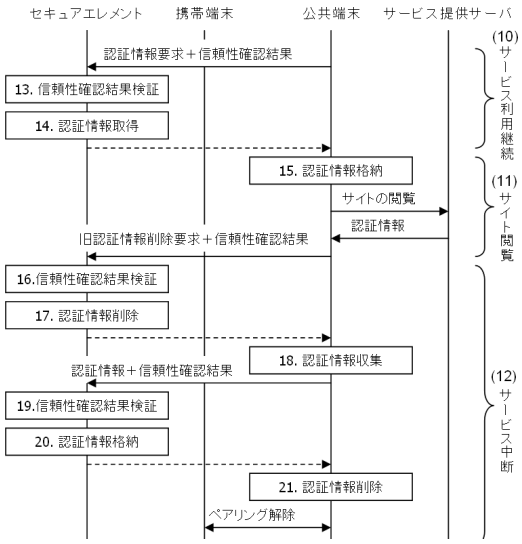

図 10 公共端末利用のシーケンス
Fig. 10 Sequence when public terminal used.

表 6 図 10 の説明
Table 6 Explanation of Fig. 10.

No.	説明
13	セキュアエレメントは，公共端末からの認証情報要求に対して，信頼性確認結果を検証する．
14	信頼性確認結果の検証に成功すれば，セキュア領域に格納している認証情報を，携帯端末を経由して公共端末に送付する．
15	公共端末は受信した認証情報を，自端末のブラウザに格納し，サービス提供サイトにアクセスする．サイトから認証情報が発行され，サービスを受ける．
16	セキュアエレメントは，公共端末からの旧認証情報削除要に対して，信頼性確認結果を検証する．
17	信頼性確認結果の検証に成功すれば，セキュア領域に格納している旧認証情報を削除する．
18	公共端末は，自端末のブラウザが管理している認証情報を収集し，携帯端末に接続されているセキュアエレメントに送付する．
19	セキュアエレメントは，公共端末からの認証情報格納要求に対して，信頼性確認結果を検証する．
20	信頼性確認結果の検証に成功すれば，セキュアエレメントは受信した認証情報をセキュア領域に書き込む．
21	公共端末は，自端末のブラウザが管理している認証情報を削除する．なお，携帯端末と公共端末間の意図せぬ通信切断を考慮して，ステップ 18 の直後に認証情報を削除することで安全性を高められる．

と，デバイス情報生成時刻を連結した情報である．デバイス情報に生成時刻を含めるのは，公共端末が不正の場合にリプレイアタックを防ぐために情報をスクランブルするためである．また，デバイス情報を暗号化するのは，公共端末にユーザの情報（セキュアエレメントの情報）を漏らさないためである．

次に，図 11 のステップ 6 で，公共端末は，署名対象元データ（自端末の端末 ID と，携帯端末から受信した暗号

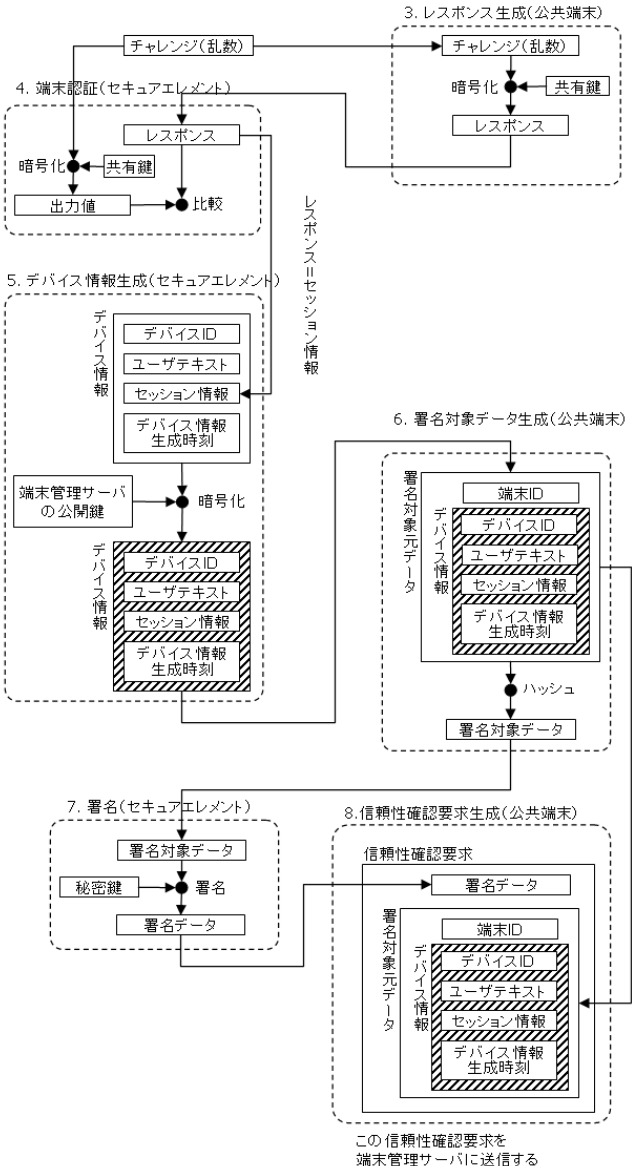

図 11 図 9 のステップ 3 からステップ 8 の詳細
Fig. 11 Details from step 3 to step 8 of Fig. 9.

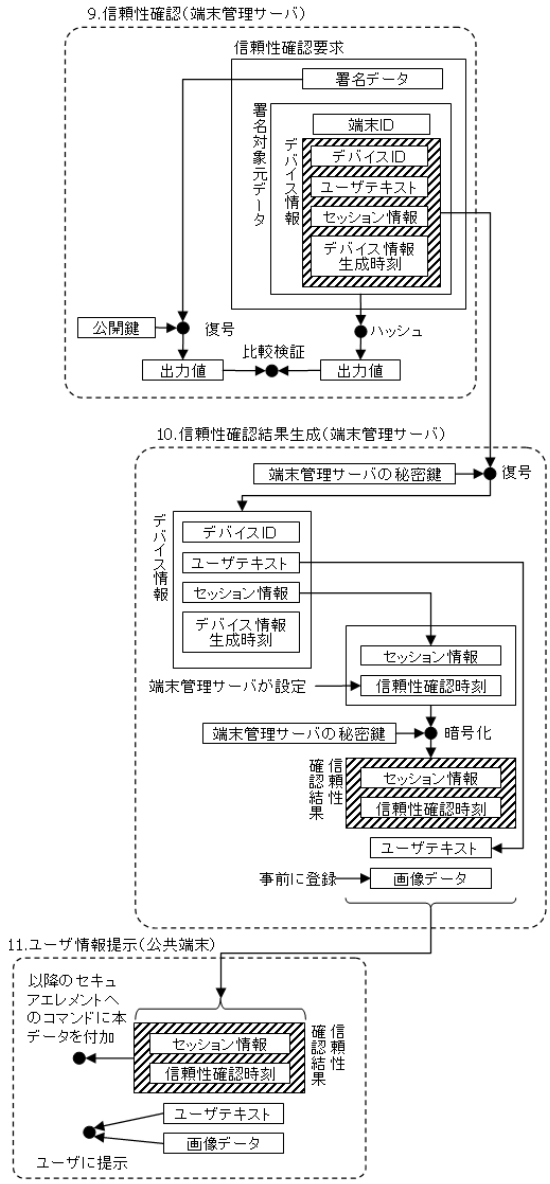

図 12 図 9 のステップ 9 からステップ 11 の詳細
Fig. 12 Details from step 9 to step 11 of Fig. 9.

化されたデバイス情報を連結したデータ）のハッシュ値（= 署名対象データ）を生成し，セキュアエレメントに送付する．ステップ 7 で，セキュアエレメントは，署名対象データを自身の秘密鍵で暗号化した署名データを生成し，公共端末に送付する．ステップ 6 の処理は，セキュアエレメント内で行ってもよいが，セキュアエレメントへのデータの転送速度や，セキュアエレメントの計算速度を考慮し公共端末側で処理を行っている．また，2.3 節の前提条件で示したように，公共端末の端末 ID は，不正の公共端末が偽造できない ID 体系により生成されているものとしている[*2]．ステップ 8 で，公共端末は端末管理サーバに対し，信頼性確認要求（ステップ 6 で生成した署名対象元データとステップ 7 で受信した署名データ）を生成し，端末管理サーバに送付する．ステップ 8 でセキュアエレメント内で生成した署名を付加しているのは，不正の第三者が勝手に信頼性確認要求を行うことを防止するためである．

次に，図 12 のステップ 9 で，端末管理サーバが受信した署名データを，その署名を生成したセキュアエレメントの秘密鍵に対応した公開鍵で検証することで，正しい信頼性確認要求であることを確認する．署名検証が成功した場合は続いて信頼性確保のインベントリ情報を確認する．インベントリ情報は，公共端末から端末管理サーバに定期的に報告されているものとしている．

署名とインベントリ情報がともに問題ないことが確認できると，図 12 のステップ 10 で，端末管理サーバは信頼性確認結果を生成する．信頼性確認結果とは，署名対象元

[*2] たとえば，チェックデジットのウェイトの計算を多重に行うことで算出計算を複雑にしたり，チェックデジットの計算方法そのものを秘匿したりすることで端末 ID の偽造は難しくなる．あるいは，公共端末の端末 ID を振番する管理団体しか知らない秘密情報を用いて暗号化した端末 ID を用いることで偽造を困難にすることができる．

データ内の暗号化されたデバイス情報を復号し，復号されたデバイス情報中のセッション情報と信頼性確認を行った時刻情報を連結し，端末管理サーバの秘密鍵で暗号化したデータである．端末管理サーバは，信頼性確認結果とユーザ情報（ユーザが事前に設定した画像データとユーザテキスト）を公共端末に送付する．

最後に，公共端末は，図 12 のステップ 11 で，端末管理サーバから受け取ったユーザ情報をユーザに提示する．ユーザは提示された情報（ユーザが事前に設定した画像データとユーザテキスト）を確認して，処理を継続するかを決定する．公共端末は，図 11 のステップ 5 でデバイス情報が暗号化されているので，目の前にいるユーザが誰なのかを知ることができないので，ユーザ情報をキャッシュして別のユーザ情報を提示しようとしてもできない．信頼性確認結果は，公共端末からセキュアエレメントへ送信される以降のコマンドに付与し，セキュアエレメント内でコマンドに付与された信頼性確認結果をそのつど確認することで不正なコマンドを排除することができる．

3.5 提案方式のモジュール構成

本節では，提案方式のモジュール構成を示す．PC 端末，携帯端末，端末管理サーバのそれぞれのモジュール構成を**図 13** に示す．

図 13 に示したように公共端末側は下記の機能モジュールで構成される．

- **GUI**：通信パラメータの設定やログの表示などを行う．
- **認証情報連携**：Bluetooth 通信を使って，携帯端末と ID/パスワードや Cookie などの認証情報の送受信を行う．
- **外部 AP 連携**：PC 上の外部アプリケーションからの認証情報の転送や削除などの命令を受け認証情報連携モジュールに伝える．
- **端末認証**：携帯端末からの要求に応じて端末認証処理を実行する．
- **信頼性確認**：端末管理サーバに，端末情報（自端末と ID デバイスの情報），および端末情報に対してセキュアエレメントが署名した署名値を送信し，信頼性確認処理を実行する．
- **インベントリ情報収集**：定期的に端末内のインストール済みソフトウェア情報などのインベントリ情報を収集し，端末管理サーバに送付する．
- **Bluetooth 通信**：FeliCa 読み込みモジュールで読み込んだ FeliCa の ID を使って携帯端末と Bluetooth のペアリングを行い携帯端末とデータの送受信を行う．
- **FeliCa 読み込み**：FeliCa がかざされるのを待ち受けて，FeliCa の ID を読み込む．
- **外部 AP**：サービスに関連した細部アプリケーション
- **ブラウザ**：Web 閲覧用のブラウザ

また，図 13 に示した携帯端末側は下記の機能モジュールで構成される．

- **GUI**：通信パラメータの設定やログの表示などを行う．
- **認証情報連携**：Bluetooth 通信を使って，PC 端末と ID/パスワードや Cookie などの認証情報の送受信を行う．
- **外部 AP 連携**：携帯端末上の外部アプリケーションからの認証情報の転送や削除などの命令を受け認証情報連携モジュールに伝える．
- **端末認証**：セキュアエレメントに接続し，認証および暗号処理を中継する．
- **Bluetooth 通信**：FeliCa の ID を使って PC と Bluetooth のペアリングを行い PC 端末とデータの送受信を行う．
- **外部 AP**：サービスに関連した細部アプリケーション
- **ブラウザ**：Web 閲覧用のブラウザ
- **FeliCa**：非接触 IC 通信を行う IC チップ
- **セキュアエレメント**：認証情報などを保管する IC チップ

さらに，図 13 に示した端末管理サーバ側は下記の機能モジュールで構成される．

- **信頼性検証**：携帯端末の署名と公共端末のインベントリ情報を検証し，検証結果とユーザ情報を公共端末に返す．
- **インベントリ情報登録**：公共端末から送付されたインベントリ情報を登録，検証する．
- **インベントリ情報提供**：登録されているインベントリ情報を提供する．

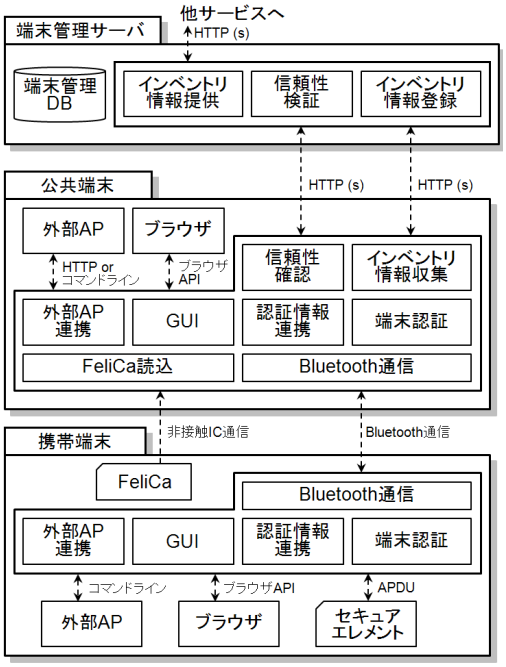

図 13 提案方式のモジュール構成
Fig. 13 Module constitution of proposal.

- **端末管理 DB**：インベントリ情報とデバイス情報を管理する．

4. 評価

本章では，端末の安全性確認処理，インベントリ情報登録関連処理の性能評価結果について記述する．

4.1 測定条件

性能測定対象の端末のスペックは，**表 7**，**表 8**，**表 9** に示したとおりである．端末間の非接触 IC 通信には FeliCa を用い，ハンドオーバ後の Bluetooth に関しては Bluetooth Ver.2.1 対応のアダプタを用いた．また，PC とサーバ間のネットワークには**表 10** に示した有線 LAN と ADSL 通信網，および CDMA 1X WIN 対応の 3G データ通信を用いた．また，計測に用いたインベントリ情報のサイズは 45 kB であった．

4.2 測定項目

以下のシーケンスを測定した．

- 携帯端末と PC 端末の連携による処理
  - **(1-1)** ID/パスワード連携によるログイン処理（図 7 の (1) 利用開始処理と (3) サイト閲覧処理）
  - **(1-2)** PC 端末から認証済み情報のセキュアエレメントへの移行処理（図 7 の (4) サービス中断処理）
- 携帯端末単体での処理
  - **(2-1)** 携帯端末単体によるログイン処理（図 8 の (5) サイト閲覧処理）
  - **(2-2)** 携帯端末内でのセキュアエレメント内の認証済み情報の削除処理（図 8 の (6) サービス中断処理の前半）
  - **(2-3)** 携帯端末内での認証済み情報のセキュアエレメントへの移行処理（図 8 の (6) サービス中断処理の後半）
- 携帯端末と公共端末の連携による処理
  - **(3-1)** 端末の安全性確認（端末認証と信頼性確認）処理（図 9 の (8) 端末認証処理と (9) 信頼性確認処理）
  - **(3-2)** 認証情報連携によるログイン処理（図 9 のステップ 1〜3 および図 10 の (10) サービス利用継続処理と (11) サイト閲覧処理）
  - **(3-3)** PC 端末からセキュアエレメント内の認証済み情報の削除処理（図 10 の (12) サービス中断処理の前半）
  - **(3-4)** PC 端末から認証済み情報のセキュアエレメントへの移行処理（図 10 の (12) サービス中断処理の後半．ただし (1-2) と同様の処理のため計測なし）
- インベントリ関連処理
  - **(4-1)** インベントリ情報の新規登録（図 9 のステップ a〜b）
  - **(4-2)** インベントリ情報の更新（図 9 のステップ a〜b（2 度目以降の場合））
  - **(4-3)** インベントリ情報の提供（図 13 の他サービスがインベントリ情報提供モジュールへ情報提供要求を送りインベントリ情報を受けるまでの処理）

表 7 測定に用いた PC 端末，公共端末のスペック
Table 7 Specification of PC terminal and public terminal used for the measurement.

OS	Windows XP SP3
CPU	Intel Core2 Duo T8100（2.10 GHz）
Memory size	3 GB
Browser	Internet Explorer 8

表 8 測定に用いた端末管理サーバのスペック
Table 8 Specification of terminal management server used for the measurement.

OS	CentOS 5.5
CPU	Intel Core2 Duo T8100（2.10 GHz）
Memory size	3 GB

表 9 測定に用いた携帯端末のスペック
Table 9 Specification of mobile terminal used for the measurement.

OS	Windows Mobile 6.5 Professional Edition
CPU	Qualcomm QSD8650 1 GHz
Memory size	512 MB（ROM）/384 MB（RAM）
Browser	Internet Explorer Mobile

表 10 測定に用いた回線スペック
Table 10 Specification of network used for the measurement.

Cable LAN	Gigabit Ethernet
ADSL	8 Mbps（downstream）1 Mbps（upstream）
3G	2.4 Mbps（downstream）114 Kbps（upstream）

4.3 測定結果

本節では，各測定項目の処理の詳細と測定結果を記載する．各測定項目において 12 回測定し，全体の時間が最小と最大のデータを除外した 10 回分の測定値から平均値を算出した．**表 11** の (1-1) より，ID パスワード連携方式で携帯端末をかざしてから 2 秒以内でログインできることが確認できた．また，(2-1) より，移動中に 3G 網を用いる携帯端末単体利用で約 10 秒で業務が継続できることが確認できた．さらに，(3-1)，(3-2) より，端末の安全性確認が必要な公共端末利用においても 10 秒以内で業務を開始できることが確認できた[*3]．

[*3] (1-2)，(2-2)，(2-3)，(3-3)，(3-4)，(4-1)，(4-2)，(4-3) はバックエンドで処理ができるステップなので，ユーザの使い勝手には影響しないようにできる．

表 11 測定結果
Table 11 Measurement results.

No.	Process	Time（Sec）
(1-1)	ID/パスワード連携によるログイン処理	1.71（LAN），1.74（ADSL）
(1-2)	PC 端末から認証済み情報のセキュアエレメントへの移行処理	4.60（Bluetooth）
(2-1)	携帯端末単体によるログイン処理	10.48（3G）
(2-2)	携帯端末内でのセキュアエレメント内の認証済み情報の削除処理	2.03（内部処理）
(2-3)	携帯端末内での認証済み情報のセキュアエレメントへの移行処理	3.03（内部処理）
(3-1)	端末の安全性確認（端末認証と信頼性確認）処理	4.35（ADSL）
(3-2)	認証情報連携によるログイン処理	5.04（LAN），5.34（ADSL），9.37（3G）
(3-3)	PC 端末からセキュアエレメント内の認証済み情報の削除処理	3.87（Bluetooth）
(3-4)	PC 端末から認証済み情報のセキュアエレメントへの移行処理	4.60（Bluetooth）
(4-1)	インベントリ情報の新規登録	0.75（ADSL）
(4-2)	インベントリ情報の更新	0.73（ADSL）
(4-3)	インベントリ情報の提供	0.95（ADSL）

5. 実運用に向けた考察

本章では，実運用に向けた考察を行う．提案方式に基づいたシステムを実際に運用する際には，公共端末にはコンビニエンスストアに設置されている「キヨスク端末」を利活用するなどが考えられる．また，空港や駅などに設置されている情報端末に適用することも可能である．

また，本提案で用いる携帯端末，PC 端末，公共端末には，専用のソフトウェアをあらかじめインストールする必要がある．携帯端末に関しては，OTA（Over the Air）でダウンロードすることも考えられる．

さらに，今回の公共端末に関する前提条件として「公共端末は，自端末のウィルスやマルウェアなどを含むインベントリ情報（ソフトウェア情報やハードウェア情報）を正しく収集し，端末管理サーバにそのインベントリ情報を正しく伝えることができるものとする」という仮定をおいた．実運用では，インベントリ情報を正しく収集するために既存のウィルスチェックソフトウェアなどを活用し，さらに，端末管理サーバに正しく情報を伝えるために，Trusted Platform Module（TPM）などのハードウェア耐タンパ機能を用いることで実現可能であると考えられる．

機能的には，実験システムを構築し，機能検証・性能検証を行い正しく動作することを検証したが，本システムを実運用に移行するためには，様々なベンダやサービス提供機関が参入できるように標準化などを推進する必要があると考える．

6. おわりに

本論文では，ユーザ認証の際に，携帯端末を「鍵」として利用する利便性と安全性を兼ね備えた認証システムを提案した．具体的には，ID/パスワードや Cookie 情報のような認証情報を携帯端末内に保管し，非接触 IC 通信と近距離無線通信を利用して，携帯端末を PC 端末にかざすだけで Web 認証が行える認証システムを提案した．また，携帯端末をかざす先の端末として，共用の公共端末を想定した場合に，その公共端末の安全性をユーザに示したうえで認証情報を連携させる方式を提案した．さらに，プロトタイプシステムを開発し，性能の評価を行った．これにより，ユーザはサービスを受ける別端末に携帯端末をかざすだけで安全に認証が行われサービスを受けることが可能となった．

今回の研究開発では，携帯端末として Windows Mobile 端末を用いてプロトタイプ実装を行った．今後は，多種多様な携帯端末の登場が予想されるために，それらの端末に対応させていく必要がある．また，携帯端末と対になる認証情報を連携させサービスを受ける側の端末としては，Windows PC 端末を用いた．今後は Windows PC 以外の Linux 端末や，タブレット型の端末の利用も想定されるために，それらの端末に対応させていく必要がある．また，携帯端末と PC 端末間の近距離無線通信として，Bluetooth 通信を用いたが，今後は，Wi-Fi や ZigBee などのような Bluetooth 以外の近距離無線通信に対応させる必要がある．さらに，今回は，ID/PW および Cookie 方式における認証情報連携機能の実装を行ったが，たとえば VPN や SSL など他のプロトコルに対応させていく必要がある．また，インベントリ情報として管理しているソフトウェアの構成を意図的に途中で変更しなくてはならない事象に対応させるために，ソフトウェアのホワイトリストなどによる運用を行う必要がある．

謝辞 本研究は，独立行政法人情報通信研究機構（NICT）の委託研究「端末プラットフォーム技術に関する研究開発」の成果の一部である．

参考文献

[1] 今井和雄，山崎憲一，中村　寛，ケレラー ヴォルフガング，倉掛正治：シームレス通信サービスとその研究開発の動向，電子情報通信学会論文誌 B，Vol.J89-B, No.8, pp.1347–1356 (2006).

[2] Schulzrinne, H. and Wedlund, E.: Application-layer mobility using SIP, *Mobile Computing and Communications Review*, Vol.4, No.3, pp.47–57 (2000).

[3] Roussopoulos, M., Maniatis, P., Swierk, E., Lai, K., Appenzeller, G. and Baker, M.: Personal-level Routing in the Mobile People Architecture, *Proc. 2nd Conference on USENIX Symposium on Internet Technologies and Systems*, Vol.2 (1999).

[4] Wang, H.J., Raman, B., Chuah, C., Biswas, R., Gummadi, R., Hohlt, B., Hong, X., Kiciman, E., Mao, Z., Shih, J.S., Subramanian, L., Zhao, B.Y., Joseph, A.D. and Katz, R.: ICEBERG: An Internet-core Network Architecture for Integrated Communications, *IEEE Personal Communications*, Vol.7, No.4, pp.10–19 (2000).

[5] 藤井亜里砂，石川清彦，森住俊美，菊地由美，山田智一，川森雅仁，川添雄彦：複数デバイス間での認証情報連携によるシームレスなコンテンツ視聴サービス，電子情報通信学会技術研究報告，MoMuC，モバイルマルチメディア通信，Vol.108, No.218, pp.21–26 (Sep. 2008).

[6] リバティアライアンス：Liberty Alliance ID-WSF 1.1 Specifications, 入手先 ⟨http://projectliberty.org/resource_center/specifications/liberty_alliance_id_wsf_1_1_specifications⟩.

[7] 梅澤克之，洲崎誠一：スマートフォンを用いたリモート接続システムの開発，第 31 回情報理論とその応用シンポジウム予稿集，pp.971–974 (Oct. 2008).

[8] 梅澤克之, 加藤崇利, 手塚　悟：携帯端末を用いた FMC 認証方式の開発, 電子情報通信学会技術研究報告 (ISEC2009-36, SITE2009-28, ICSS2009-50), pp.203–208 (July 2009).

[9] 梅澤克之，加藤崇利，手塚　悟：スマートフォンを用いたリモート接続システムの開発と評価，第 8 回情報科学技術フォーラム（FIT2009）予稿集第 4 分冊，pp.67–73 (Sep. 2009).

[10] 梅澤克之，手塚　悟：スマートフォンをセキュアデバイスとして用いるリモート接続システムの開発と評価，電子情報通信学会論文誌 B，Vol.J94-B, No.4, pp.530–538 (2011).

[11] 梅澤克之，田代　卓，手塚　悟：GBA プロトコルに基づいた認証情報連携技術の開発と評価，電子情報通信学会技術研究報告，Vol.110, No.113, pp.47–53 (July 2010).

[12] 梅澤克之，加藤崇利，田代　卓：認証済み Cookie 情報の端末間での連携技術の開発と評価，コンピュータセキュリティシンポジウム（CSS2009）予稿集，pp.81–86 (Oct. 2009).

[13] Umezawa, K., Tashiro, T. and Tezuka, S.: A Proposal for Federation Technology for authenticated information Between Terminals, *International Conference on Mobile, Ubiquitous and Pervasive Computing* (*ICMUPC 2010*), World Academy of Science, Engineering and Technology, Vol.63, pp.277–284 (Mar. 2010).

[14] 梅澤克之，手塚　悟：携帯電話を認証情報の保管庫として用いる端末連携認証システムの提案，電子情報通信学会技術研究報告，Vol.110, No.290, pp.73–78 (Nov. 2010).

梅澤 克之　（正会員）

1996 年早稲田大学大学院理工学研究科機械工学専攻修士課程修了．同年（株）日立製作所入社．以来システム開発研究所（現：横浜研究所）にて，分散オブジェクトシステム，モバイルセキュリティ技術，スマートカードセキュリティ技術等の研究・開発に従事．2012 年より同社情報システム事業部にて仮想化技術の研究・開発に従事．2010 年よりサイバー大学客員研究員，2010 年より湘南工科大学非常勤講師を兼務．電子情報通信学会，電気学会各会員．博士（工学）．

礒川 弘実　（正会員）

1996 年九州大学大学院工学研究科知能システム学専攻修士課程修了．同年（株）日立製作所入社．以来システム開発研究所（現：横浜研究所）にて，ネットワーク管理技術，セキュリティ管理技術等の研究・開発に従事．

加藤 崇利　（正会員）

1995 年早稲田大学大学院理工学研究科電気工学専攻修士課程修了．同年（株）日立製作所入社．以来システム開発研究所（現：横浜研究所）にて，光ディスク装置の符号化，スマートカードセキュリティ，デスクトップ仮想化技術等の研究・開発に従事．IEEE，電子情報通信学会各会員．

萱島 信 （正会員）

1989 年横浜国立大学大学院工学研究科電子情報工学専攻博士課程前期修了．同年（株）日立製作所入社．以来システム開発研究所（現：横浜研究所）にて AI 技術，オブジェクト指向技術，ネットワーク技術，セキュリティ技術等の研究に従事．現在，同研究所主任研究員．2006 年より IPA セキュリティセンター情報セキュリティ技術ラボラトリー研究員を兼務．電子情報通信学会，AI 学会各会員．博士（工学）．

手塚 悟 （正会員）

2009 年度より，東京工科大学コンピュータサイエンス学部の教授，現在に至る．1984 年度より，（株）日立製作所入社．マイクロエレクトロニクス機器開発研究所に勤務し，パーソナルコンピュータのオペレーティングシステム，デバイスドライバ，LAN システム等の研究開発に従事．その後，システム開発研究所に勤務し，パーソナルコンピュータを中心とした LAN システムの構築・運用管理の研究開発，さらに電子政府，電子自治体等を主に情報セキュリティシステムの研究開発に従事．特に，PKI 技術を用いた電子署名，電子認証等の研究．慶應義塾大学理工学部特別講師，大阪大学非常勤講師等歴任．2004 年度情報処理学会論文賞，2008 年度情報処理学会論文賞，IEEE-IIHMSP2006 Best Paper Award．工学博士．著書に『Inside CORBA』アスキー出版（共訳，1998 年），『インターネットコマース—新動向と技術』共立出版（共著，2000 年），『インターネット時代の情報セキュリティー—暗号と電子透かし』共立出版（共著，2000 年），『情報セキュリティの基礎』共立出版（編著，2011 年）．